JOURNAL OF NUMBER THEORY 3, 7–12 (1971)

Pure Cubic Fields whose Class Numbers are Multiples of Three

TAIRA HONDA

Department of Mathematics, Osaka University, Toyonaka, Osaka 560, Japan

Communicated by Y. Kawada

Received February 20, 1970

The author determines all pure cubic fields $\mathbf{Q}(\sqrt[3]{n})$ whose class numbers are multiples of three.

1. STATEMENT OF RESULTS

In this article we determine all pure cubic fields whose class numbers are multiples of three.

Let $n \neq 1$ be a cube-free natural number and put $\Omega = \mathbf{Q}(\sqrt[3]{n})$. Then Ω is a cubic extension of $\mathbf{Q}$, its normal closure L equals $\Omega(\zeta)$ where $\zeta = \exp(2\pi i/3)$, and the Galois group $G = G(L/\mathbf{Q})$ is isomorphic to the symmetric group of degree three. Let σ be an element of order three in G and τ be the complex conjugacy of L. Then $K = \mathbf{Q}(\zeta)$ (resp. Ω) is the subfield of L, consisting of numbers fixed by σ (resp. τ).

Denote by h_Ω (resp. h_L) the class number of Ω (resp. L) and by $a_{L/K}$ the number of ambigous classes for the cyclic extension L/K. Then $3 \mid h_\Omega \Leftrightarrow 3 \mid a_{L/K}$ by the following two lemmas:

LEMMA 1. *$h_L = h_\Omega^2$ or $h_L = \frac{1}{3}h_\Omega^2$.*

LEMMA 2. *$3 \mid h_L \Leftrightarrow 3 \mid a_{L/K}$.*

The proof of Lemma 1 will be given in Section 2. Lemma 2 is a special case of a well-known fact. (A short proof of Lemma 2: Decompose the Sylow 3-subgroup of the ideal class group of L into the union of orbit sets relative to $G(L/K)$.)

Now we see by Theorem 13 of Hasse [3] that

$$a_{L/K} = 3^{e-t-1},$$

where e is the number of prime ideals of K which are ramified in L and $t = 0$ or 1 according as $\zeta \in N_{L/K}L^*$ or not. Hence $3 \mid a_{L/K}$ whenever

$e \geqslant 3$ and $3 \nmid a_{L/K}$ if $e = 1$. For $e = 2$ we can determine the value of t in all cases by using the properties of the norm residue symbol. The result is as follows:

THEOREM. *The class number h_Ω is not a multiple of three if and only if n has one of the following forms*:

(i) $n = 3$;

(ii) $n = p$, *where p is a prime number such that* $p \equiv -1 \pmod 3$;

(iii) $n = 3p$ *or* $9p$, *where p is a prime number such that* $p \equiv 2$ *or* $5 \pmod 9$;

(iv) $n = pq$, *where p and q are prime numbers such that* $p \equiv 2$ *and* $q \equiv 5 \pmod 9$;

(v) $n = p^2q$, *where p and q are distinct prime numbers such that* $p \equiv q \equiv 2$ *or* $5 \pmod 9$.

(Since $\mathbf{Q}(\sqrt[3]{a^2b}) = \mathbf{Q}(\sqrt[3]{ab^2})$, we have counted only one of $n = a^2b$ and $n' = ab^2$.)

If $3 \mid h_\Omega$, there is a cubic, cyclic, and unramified extension of Ω by class field theory. In fact we can construct such an extension explictly in case n has a prime divisor p such that $p \equiv 1 \pmod 3$(cf. Section 4).

2. PROOF OF LEMMA 1

For a subfield k of L, denote by χ_K the character of G induced by the principal character of $G(K/k)$. Since

$$\chi_L - \chi_\mathbf{Q} = \chi_K - \chi_\mathbf{Q} + 2(\chi_\Omega - \chi_\mathbf{Q}), \tag{1}$$

as is easily verified, we get

$$h_L R_L = h_\Omega^2 R_\Omega^2 \tag{2}$$

by the formula (12) of Kuroda [5] or Brauer [2], where R_k denotes the regulator of k. Let $\epsilon > 1$ be a fundamental unit of Ω. For any unit E of L, $|E|^2 = E^{1+\tau}$ is a unit of Ω and hence a power of ϵ. Therefore $R_L/R_\Omega^2 = R_L/(\log|\epsilon|)^2$ is a rational integer. On the other hand, since $|\epsilon^{1+\sigma+\sigma^2}| = 1$ and $|\epsilon^\sigma| = |\epsilon^{\sigma\tau}| = |\epsilon^{\tau\sigma^2}| = |\epsilon^{\sigma^2}|$ we have

$$|\epsilon||\epsilon^\sigma|^2 = |\epsilon||\epsilon^{\sigma^2}|^2 = 1.$$

Therefore

$$R[\epsilon, \epsilon^{\sigma}] = \begin{vmatrix} 2\log|\epsilon| & 2\log|\epsilon^{\sigma}| \\ 2\log|\epsilon^{\sigma}| & 2\log|\epsilon^{\sigma^2}| \end{vmatrix}$$

$$= \begin{vmatrix} 2\log|\epsilon| & -\log|\epsilon| \\ -\log|\epsilon| & -\log|\epsilon| \end{vmatrix}$$

$$= -3(\log|\epsilon|)^2,$$

which implies that $3R_{\Omega}^2/R_L$ is a rational integer. Hence we must have

$$R_L = R_{\Omega}^2 \quad \text{or} \quad R_L = 3R_{\Omega}^2. \tag{3}$$

Of course Lemma 1 is a direct consequence of (2) and (3).

3. Proof of the Theorem

Let $\mathfrak{l}$ be the prime ideal of K which divides three. By Theorem 9 of Ref. [3] $\mathfrak{l}$ is unramified in L if and only if $n \equiv \pm 1 \pmod 9$. Denote by $(\ ,\ /p)$ the cubic Hilbert symbol in K. (See Hasse [4] or Artin–Tate [1] for its basic properties.) As is well-known, $\zeta \in N_{L/K}L^*$ if and only if

$$\left(\frac{\zeta, n}{\mathfrak{p}}\right) = 1 \tag{4}$$

for all prime ideal $\mathfrak{p}$ of K. Since ζ is a unit, (4) holds whenever $\mathfrak{p}$ is unramified in L. Moreover, in the only nontrivial case $e = 2$ we have only to check (4) for one ramified prime ideal $\mathfrak{p}$ because of the product formula of the Hilbert symbol. The case $e = 2$ may happen only if n is a prime number or has two prime factors.

(I). *The case n is a prime number p.*

For $p = 3$ we have $e = 1$. If $p \equiv 1 \pmod 9$, then $e = 2$ since (p) decomposes in K and $\mathfrak{l}$ is unramified in L. Let $\mathfrak{p}$ be a prime divisor of (p) in K. Then

$$\left(\frac{\zeta, p}{\mathfrak{p}}\right) = \left(\frac{p, \zeta}{\mathfrak{p}}\right)^{-1} = 1,$$

since $\mathfrak{p}$ decomposes completely in $K(\sqrt[3]{\zeta}) = \mathbf{Q}(\exp(2\pi i/9))$. Hence $t = 0$ in this case, so that $a_{L/K} = 3$. If $p \equiv 4$ or $7 \pmod 9$, then $e = 3$. If $p \equiv -1 \pmod 9$, (p) remains prime in K and $e = 1$. Assume finally

$p \equiv 2$ or $5 \pmod 9$. Then only (p) and $\mathfrak{l}$ are ramified in L/K. By Theorem 10 of Ref. [1], Chapter 12, we have

$$\left(\frac{\zeta, p}{\mathfrak{l}}\right) = \left(\frac{\zeta, -p}{\mathfrak{l}}\right) = \zeta^{\frac{1}{3}S(\log(-p))} \neq 1,$$

so that $t = 1$ and $a_{L/K} = 1$. Summing up, we have $3 \mid a_{L/K}$ if and only if $n = p \equiv 1 \pmod 3$.

(II). *The case n has two prime factors p and q*

A. *The case $n = 3p$ or $9p$*

In this case $e = 2$ if and only if $p \equiv -1 \pmod 3$. We have

$$\left(\frac{\zeta, 3}{\mathfrak{l}}\right) = \left(\frac{\zeta, 1-\zeta}{\mathfrak{l}}\right)\left(\frac{\zeta, 1-\zeta^2}{\mathfrak{l}}\right)$$
$$= \left(\frac{\zeta^2, 1-\zeta^2}{\mathfrak{l}}\right)^{-1} = 1.$$

Therefore

$$\left(\frac{\zeta, n}{\mathfrak{l}}\right) = \left(\frac{\zeta, p}{\mathfrak{l}}\right),$$

which equals 1 if and only if $p \equiv -1 \pmod 9$ everywhere. Thus we get case (iii) of our Theorem.

Assume $p \neq 3$ and $q \neq 3$. Then $e = 2$ if and only if $n \equiv \pm 1 \pmod 9$ and $p \equiv q \equiv -1 \pmod 3$. As is easily verified, the following three cases are possible:

B. *The case $n = pq$, where $p \equiv 2$ and $q \equiv 5 \pmod 9$*

We have

$$\left(\frac{\zeta, n}{p}\right) = \left(\frac{\zeta, p}{p}\right)\left(\frac{\zeta, q}{p}\right) = \left(\frac{\zeta, p}{p}\right) = \left(\frac{p, \zeta}{p}\right)^{-1}.$$

Since (p) remains prime in $K(\sqrt[3]{\zeta})$, it holds $(p, \zeta/p) \neq 1$, so that $t = 1$.

C. *The case $n = pq$, where $p \equiv q \equiv -1 \pmod 9$*

Since (p) decomposes completely in $K(\sqrt[3]{\zeta})/K$, we have

$$\left(\frac{\zeta, n}{p}\right) = \left(\frac{\zeta, p}{p}\right)\left(\frac{\zeta, q}{p}\right)$$
$$= \left(\frac{\zeta, p}{p}\right) = \left(\frac{p, \zeta}{p}\right)^{-1} = 1,$$

so that $t = 0$.

D. *The case* $n = p^2q$ *where* $p \equiv q \equiv -1 \pmod 3$ *and* $p \equiv q \pmod 9$

By the same argument as in Cases B and C we see $t = 1$ if and only if $p \equiv q \equiv 2$ or $5 \pmod 9$.

This settles all possible cases and completes the proof of our Theorem.

4. Explicit Construction of an Unramified Extension

In this section we assume that n has a prime factor p with $p \equiv 1 \pmod 3$.

Proposition 1. *For any prime number* p *such that* $p \equiv 1 \pmod 3$, *there are* $a, b \in \mathbf{Z}$ *such that* $p = (a^2 + 27b^2)/4$. *Moreover, let* α *be a root of the cubic equation*

$$X^3 - pX + pb = 0. \tag{5}$$

Then $\mathbf{Q}(\alpha)$ *is the cubic subfield of* $\mathbf{Q}(\exp(2\pi i/p))$.

Proof. Since $p \equiv 1 \pmod 3$, there exists an integer β in K such that $N_{K/\mathbf{Q}}\beta = p$. Multiplying β by ζ or ζ^2 if necessary, we may assume that β has the form $(a + 3(-3)^{1/2}b)/2$, which implies $p = (a^2 + 27b^2)/4$. The discriminant of Eq. (5) is

$$\begin{aligned} 4p^3 - 27p^2b^2 &= p^2(4p - 27b^2) \\ &= (ap)^2, \end{aligned}$$

which is a perfect square. Hence $\mathbf{Q}(\alpha)$ is a cubic, cyclic extension of $\mathbf{Q}$ unless all roots of (5) are rational. But if all roots of (5) were rational integers, they must have been multiples of p, so that $p^3 \mid pb$, a contradiction. Now let q be a prime number which is ramified in $\mathbf{Q}(\alpha)$. Then there exists $h \in \mathbf{Z}$ such that

$$X^3 - pX + pb \equiv (X - h)^3 \pmod q. \tag{6}$$

Comparing both sides of (6) we see easily that (6) holds only if $q = p$. Hence $\mathbf{Q}(\alpha)$ is contained in $\mathbf{Q}(\exp(2\pi i/p))$ and its (unique) cubic subfield. This completes our proof.

Proposition 2. *Assumptions and notations being as above,* $\Omega(\alpha)$ *is a cubic, unramified extension of* Ω.

Proof. We have only to prove that prime divisors of p in Ω are unramified in $\Omega(\alpha)$. Let $\mathfrak{P}$ be a prime divisor of p in $L(\alpha)$ and T the interia group of $\mathfrak{P}$ relative to $L(\alpha)/\mathbf{Q}$. If a prime divisor of p in Ω were ramified

in $\Omega(\alpha)$, T would have order nine. Since $\mathfrak{P}$ is tamely ramified, T must have been a cyclic group of order nine. But this is impossible, because $G(L(\alpha)/\mathbf{Q})$ is isomorphic to a subgroup of $G(L/\mathbf{Q}) \times G(\mathbf{Q}(\alpha)/\mathbf{Q})$. This completes the proof of our Proposition.

Added in proof. The "only if" part of our Theorem was already proved in a recent paper of P. Barrucand and H. Cohn; A Rational Genus, Class Number Divisibility, and Unit Theory for Pure Cubic Fields, This Journal **2** (1970), 7–21.

References

1. E. Artin and J. Tate, "Class Field Theory," Harvard Univ. Press, Cambridge, Mass. 1961.
2. R. Brauer, Beziehungen zwischen Klassenzahlen von Teilkörpern eines galoisschen Körpers, *Math. Nachr.* **4** (1951), 158–174.
3. H. Hasse, Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, $\mathbf{I}_a'$, *Jber. Deutsch. Math.-Verein.* **36** (1927), 255–311.
4. H. Hasse, Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, II, *Jber. Deutsch. Math.-Verein.* **39** (1930), 1–204.
5. S. Kuroda, Über die Klassenzahl algebraischer Zahlkörper, *Nagoya Math. J.* **1** (1950), 1–10.